IT-Sicherheit –
Die notwendige Einschaltung von Betriebsrat und Personalrat

von Wolfgang Däubler

Cyberangriffe auf Unternehmen haben in den letzten Jahren weiter zugenommen. Dem Bundeskriminalamt wurden 2022 insgesamt 136.865 Fälle gemeldet, doch sei dies nach seiner Einschätzung nur die Spitze des Eisbergs: Lediglich etwa ein Zehntel aller Fälle würden bekannt. Auch seien die aus dem Ausland kommende Angriffe in der Statistik nicht erfasst.[1] Eine verbreitete Angriffsform besteht darin, dass durch Schadsoftware das ganze System eines Unternehmens lahmgelegt wird und dieses anschließend eine „Mitteilung" erhält, bei Zahlung der Summe X (meist in Bitcoins) werde alles wieder frei geschaltet; andernfalls sei es definitiv verloren. Häufig muss man auch mit einem sog. Phishing rechnen: Im Anhang zu einer harmlos aussehenden Mail der (angeblichen) Hausbank findet sich z. B. ein Fragebogen, in dem man „zu Verifikationszwecken" zahlreiche Kontodaten eintragen soll, die dann zum „Abräumen" des Kontos verwendet werden.[2]

Es versteht sich von selbst, dass sich Unternehmen gegen solche Erpressungen schützen wollen. Bei staatlicher oder privater Infrastruktur besteht noch das weitere Problem, dass bei Angriffen u.U. elementare Bedürfnisse der Bevölkerung nicht mehr befriedigt werden können: Wenn das Wasserwerk oder das Krankenhaus plötzlich ohne IT dasteht, kann dies verheerende Folgen haben.[3]

Sicherheitsvorkehrungen

Welche Schutzmaßnahmen ergriffen werden, ist nicht im Einzelnen rechtlich geregelt. Das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)[4] enthält in den §§ 8a bis 8i lediglich allgemeine Vorgaben, die viel Konkretisierungsspielraum lassen. Außerdem gilt das BSI-Gesetz nur für die sog. kritische Infrastruktur wie Energieversorger,

[1] https://www.tagesschau.de/inland/cyberangriffe-deutschland-bka-100.html (abgerufen am 10.11.2023)
[2] Zum Phishing s. https://www.bundespolizei-virus.de/it-sicherheit/phishing/ (abgerufen am 10.11.2023)
[3] S. Konrad-Klein, CuA 2/2017 S. 24: In einem Krankenhaus in Neuss war fast einen Tag lang kein Zugriff auf die Systeme möglich; Einblick in Patientenunterlagen sowie die Vorbereitung und Durchführung von Operationen waren ausgeschlossen.
[4] vom 14. August 2009, BGBl I S. 2821, zuletzt geändert durch Art. 12des Gesetzes vom 23. Juni 2021, BGBl I S. 1982

Krankenhäuser usw., nicht aber für alle Unternehmen.[5] Die übrigen Unternehmen orientieren sich an den (rechtlich nicht verbindlichen) ISO-Normen 27001 ff. oder – wenn sie sich gegen IT-Risiken versichern wollen – an den Richtlinien der Versicherungswirtschaft. Man kann sich des Eindrucks nicht erwehren, dass die heute bestehende Rechtsordnung sehr viel mehr Wert legt auf die Sicherung personenbezogener Daten (Art. 32 DSGVO) als auf den Schutz der Allgemeinheit und selbst auf den Schutz der Integrität von Unternehmen. Dies mag einer individualistischen Denkweise entspringen, die den „Dichter und Denker" und seine Persönlichkeit umfassend schützen will, ohne darauf zu achten, dass auch er wie alle anderen Menschen Lebensumstände braucht, in denen zumindest die „basic needs" wie Wasser, Strom, Wohnung und Nahrung gesichert sind.

Mitbestimmung bei fehlenden zwingenden Vorgaben

Für die Mitbestimmung des Betriebsrats und des Personalrats ergeben sich mehr Anwendungsmöglichkeiten, wenn keine zwingenden gesetzlichen Vorgaben vorhanden sind. Dabei hängt die Entscheidung, ob die Voraussetzungen eines Mitbestimmungsrechts gegeben sind, von den jeweiligen Umständen des Einzelfalls ab.

Einschlägige Rechtsprechung ist bislang spärlich. Das Arbeitsgericht Düsseldorf hatte über einen Fall zu entscheiden, bei dem die Arbeitgeberin eine dreizehnminütige Schulung zum Sicherheitsbewusstsein „zum Schutze der IT" durchführen wollte.[6] Arbeitgeber und Betriebsrat waren sich einig, dass hierfür ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 1 BetrVG bestehe, was vom Arbeitsgericht Düsseldorf im Rahmen eines Verfahrens nach § 100 ArbGG bestätigt wurde. Auch das LAG Düsseldorf hatte als Beschwerdeinstanz insoweit keine Bedenken.[7]

Von grundsätzlicherer Bedeutung war demgegenüber eine Entscheidung des LAG München.[8] Dabei ging es um den Einsatz des Systems „Securonix", das Abweichungen vom normalen Nutzungsverhalten, sog. Auffälligkeiten, erkennen kann. Dabei werden Logdaten erfasst, die sich auf einzelne Mitarbeiter beziehen lassen. Die Auswertung kann ergeben, dass es sich um einen harmlosen Zufall handelte, der keine weitere Aufmerksamkeit erfordert. Es kann aber

[5] Einzelheiten bei Däubler, Digitalisierung und Arbeitsrecht, 8. Aufl., Frankfurt/Main 2022, § 19 Rn.5 ff., auch zum Folgenden
[6] ArbG Düsseldorf, 5.3.2018 – 15 BV 38/18
[7] LAG Düsseldorf, 8.5.2018 – 3 TaBV 15/18 – LAGE § 76 BetrVG 2001 Nr. 9
[8] LAG München 23.7.2020 – 2 TaBV 126/19.

auch ein Ausnahmeverhalten vorliegen, das für sich allein kein erhöhtes Risiko indiziert, aber im Wiederholungsfalle Relevanz gewinnt. Weisen Auffälligkeiten auf eine ernste Bedrohung hin, hat eine eingehende Untersuchung im Rahmen eines „Incident Management“ - Prozesses zu erfolgen. Das LAG München bejahte ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG, da das System geeignet war, Verhalten und Leistung von Arbeitnehmern zu kontrollieren.

In der Sache selbst wurde durch einen Mehrheitsbeschluss der mit dem Fall befassten Einigungsstelle das System gebilligt, weil zwar ein weitgehender Eingriff in die Persönlichkeitssphäre vorliege, dieser jedoch zur Schaffung von IT-Sicherheit geeignet und erforderlich sei und keine unverhältnismäßige Maßnahme darstelle. Dies war insoweit bedenklich, als die betroffenen Arbeitnehmer nicht voll darüber aufgeklärt wurden, nach welchen Kriterien die erhobenen Daten ausgewertet, d. h. als normal oder „auffällig“ qualifiziert wurden. Auch ist die Frage zu stellen, ob es nicht mildere Mittel wie eine stichprobenweise Erfassung gibt, die aus verfassungsrechtlichen Gründen den Vorrang hätten. Auch liegt der Sache nach ja eine Überwachung ohne konkreten Verdacht vor, was zumindest einer ganz besonders starken Rechtfertigung bedarf.[9]

Aus der Personalvertretung sind keine einschlägigen Entscheidungen ersichtlich. Die Voraussetzungen für ein „Mitbestimmungsrecht“ nach § 80 Abs. 1 Nr. 21 BPersVG sind keine anderen als die des § 87 Abs. 1 Nr. 6 BetrVG, doch kann die Einigungsstelle nach § 75 Abs. 3 BPersVG nur eine Empfehlung an die Oberste Dienstbehörde beschließen (weshalb das Wort „Mitbestimmungsrecht“ auch in Anführungszeichen gesetzt ist). Immerhin besteht nach § 77 Abs. 2 Nr. 1 BPersVG ein Initiativrecht des Personalrats, das allerdings in dieselbe Sackgasse führt.

Initiativen der betrieblichen Interessenvertretung?

Für IT-Sicherheit zu sorgen, ist keine ausdrücklich dem Betriebsrat oder dem Personalrat zugewiesene Aufgabe. Dies hängt damit zusammen, dass es sich jedenfalls im Anwendungsbereich des BSI-Gesetzes primär um (auch) im Allgemeininteresse bestehende Sicherungsmaßnahmen handelt, die ähnlich wie im Polizeirecht dem öffentlichen Recht zugeordnet sind und ggf. durch Verwaltungsakt des Bundesamts für die Sicherheit in der

[9] Kritisch deshalb Wedde, jurisPR-ArbR 17/2021 Anm. 6

Informationstechnik (BSI) durchgesetzt werden können. Das bedeutet allerdings nicht, dass eine betriebliche Interessenvertretung die Augen vor entsprechenden Gefahren schließen sollte. Die Situation ist insoweit keine andere als im Umweltrecht, das in der Betriebsverfassung bis 2001 ebenfalls keine Erwähnung fand, aber trotzdem im Rahmen der Qualifizierung nach § 37 Abs. 6 und 7 BetrVG[10] und im Rahmen des Bezugs von Zeitschriften nach § 40 BetrVG[11] Bedeutung gewann. Für den Betriebsrat wie für den Personalrat ergeben sich zwei Aufgabenfelder.

Die Beschäftigten wissen häufig sehr viel besser als ihre obersten Chefs, wo Gefahren lauern können. Nach der Störfall-Verordnung (die insbesondere auf Chemie-Unternehmen Anwendung findet) müssen deshalb vor der Aufstellung eines Alarm- und Gefahrenabwehrplanes die Beschäftigten des betroffenen Betriebsbereichs angehört werden – ihr „Gefahrenwissen" soll berücksichtigt werden.[12] Betriebsrat und Personalrat können anregen, dass bei der IT-Sicherheit in gleicher Weise verfahren wird. Dabei können sie sich auf § 80 Abs. 1 Nr. 2 BetrVG bzw. § 62 Nr. 1 BPersVG stützen, wonach sie Maßnahmen beantragen können, die dem Betrieb bzw. der Dienststelle dienen – das kann unschwer auf die IT-Sicherheit bezogen werden. Eine solche Initiative setzt einen guten Informationsstand voraus – die § 80 Abs. 2 BetrVG bzw. § 66 Abs. 1 BPersVG räumen der Interessenvertretung das Recht ein, alle Informationen zu erhalten, die sie zur Erfüllung ihrer Aufgaben benötigen. Die Initiative kann sich selbstredend nicht nur darauf beschränken, die Beschäftigten zu befragen; möglich sind auch Vorschläge zum Ankauf einer bestimmten Schutzsoftware und zur Schaffung eines „Reserveservers", der neben dem offiziellen System steht und jeden Abend den neuesten Stand der Dinge speichert.

Der Betriebsrat und der Personalrat werden außerdem darüber wachen, ob Sicherungssysteme eingeführt werden, die einzelne Mitbestimmungsrechte berühren. Sobald personenbezogene Daten betroffen sind, kommt das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG ins Spiel – dabei ist insbesondere zu prüfen, ob die geplante Maßnahme auf einer zwingenden gesetzlichen Vorgabe beruht oder ob der Arbeitgeber über Spielräume verfügt. Im Einzelfall kann auch § 87 Abs. 1 Nr. 1 BetrVG bzw. § 80 Abs. 1 Nr. 18 BPersVG berührt sein, weil z. B. bestimmte Regeln über das Verhalten im Betrieb aufgestellt werden, die sich nicht

[10] ArbG Wiesbaden, 2.10.1991 – 7 BV 6/91 – AiB 91, 540: Gegenstand einer Schulung nach § 37 Abs. 6; BAG, 11.10.1995 – 7 ABR 42/94 – NZA 1996, 934, 937: Gegenstand einer Schulung nach § 37 Abs. 7

[11] LAG Frankfurt/Main, 21.3.1991 – 12 TaBV 191/90 – NZA 1991, 859 = AiB 1991, 335: Bezug der Zeitschrift „Arbeit & Ökologie-Briefe".

[12] Kohte, in: Handkommentar BetrVG, 6. Aufl., Baden-Baden 2022, § 87 Rn.91

zwingend aus der Ausführung der Arbeit ergeben. Weiter ist auch an § 87 Abs. 1 Nr. 12 BetrVG bzw. § 80 Abs. 1 Nr. 14 BPersVG zu denken, die ein Initiativ- und Mitbestimmungsrecht bei Verbesserungsvorschlägen vorsehen. Warum sollten sich diese nicht auf die IT-Sicherheit erstrecken können?

Der IT-Sicherheitsbeauftragte

In vielen Betrieben wird ein „Informationssicherheitsbeauftragter" bestellt, der anders als der betriebliche Datenschutzbeauftragte keine Erwähnung im Gesetz gefunden hat.[13] Seine Aufgaben ergeben sich aus Regelwerken wie ISO 27002 oder dem BSI-Standard 200-2, die rechtlich nicht verbindlich sind, aber faktisch weithin befolgt werden. Im vorliegenden Zusammenhang interessiert, inwieweit der Betriebsrat bzw. Personalrat bei seiner Bestellung eingeschaltet ist.

Wird ein bisher im Betrieb beschäftigter Arbeitnehmer zum IT-Sicherheitsbeauftragten bestellt, so ändert sich damit sein Tätigkeitsfeld. In der Regel liegt dann ähnlich wie bei der Bestellung zum betrieblichen Datenschutzbeauftragten eine Versetzung vor, die dem Betriebsrat ein Zustimmungsverweigerungsrecht nach § 99 Abs. 2 BetrVG gibt. Fehlt der betroffenen Person die nötige Fachkunde, wäre dies ein ausreichender Grund für ein „Nein". Ein unzulässiger Interessenkonflikt würde vorliegen, wenn der betriebliche Datenschutzbeauftragte zum IT-Sicherheitsbeauftragten bestellt werden soll: In der ersten Rolle müsste er dafür sorgen, dass möglichst wenige Daten erhoben und verarbeitet werden, in der zweiten Rolle ist er an möglichst umfassenden Informationen über alles interessiert, was im Betrieb geschieht. Deshalb darf es keine „Personalunion" geben. In der Personalvertretung des Bundes ist die Situation keine prinzipiell andere.[14]

Auch die IT-Sicherheit gehört zu den Aufgaben des Betriebsrats und des Personalrats. Er kann hier einiges bewirken.

[13] Eingehend dazu Däubler, in: Kipker (Hrsg.), Cybersecurity. Rechtshandbuch, 2. Aufl., München 2023, Kap. 12 Rn.113 ff.
[14] § 78 Abs. 1 Nr. 2 bis 6 BPersVG